Exhibit 13

SW-SEC00043618

From: Pierce, Kellie [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0150EF14C7A24CB1A0E08EC9FCB06424-PIERCE, KEL]
Sent: 1/8/2018 11:34:09 PM
To: Cline, Brad [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c1da7afa0bce413f9c32ce66040660f3-Cline, Brad]; Taylor, Brody [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=71bea8d4ba2b4cf987d83d5ca8710846-Taylor, Bro]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]; Mills, David [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=39807570d2924680b3129f6920f14824-Mills, Davi]; Holmberg, Rick [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a3c5e69002674a9e93947be117d2ea15-Holmberg, R]; Dougherty, Brian [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2dac9b221993426a83b0ab0518aee0c1-Dougherty,]
CC: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject: User Access Management
Attachments: 20180104 Access Management Options.pptx

Hello everyone,
Please find the presentation for this week's User Access Management meeting (scheduled for 1/11/18).

The presentation contains the following information:

- Problem statement
- An overview of tools evaluated and evaluation criteria
- Recommendation - I've drafted a recommendation of using Azure and leveraging SharePoint workflow, based on the last meeting's discussion. ***PLEASE REVIEW***

As we discussed, each of the 5 tools were scored and here are the final scores:

Requirement (Desired Response) [Points for DR]	API friendly (Y) [2]	Identity Mgmt. (Y) [5]	Role Mgmt. (Y) [5]	Permission Workflow (Y) [5]	Privileged Access (Y) [5]	Audit Reporting (Y) [5]	Non-AD friendly (Y) [3]	Additional License Cost (N) [3]	External Development (Y) [1]	In-house Development (Y) [1]	Total Tool Points
Azure	Y(2)	Y(5)	Y(5)	Y(5)	Y(5)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	35
OKTA	Y (2)	Y (5)	Y (5)	N (0)	Y (5)	Y (5)	Y (3)	N (3)	Y (1)	Y (1)	30
SWIPE/GaTor Tool Concept	Y(2)	N(0)	N(0)	Y(5)	N(0)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	25
Thycotic	N(0)	Y(5)	Y(5)	N(0)	Y(5)	Y(5)	Y(3)	Y(0)	Y(1)	Y(1)	25
Web Help Desk	N(0)	N(0)	N(0)	N(0)	N(0)	Y(5)	Y(3)	N(3)	N(0)	Y(1)	12

Total Available Points	%
35	100%
35	86%
35	71%
35	71%

35	34%

Feel free to send me updates needed prior to the meeting.

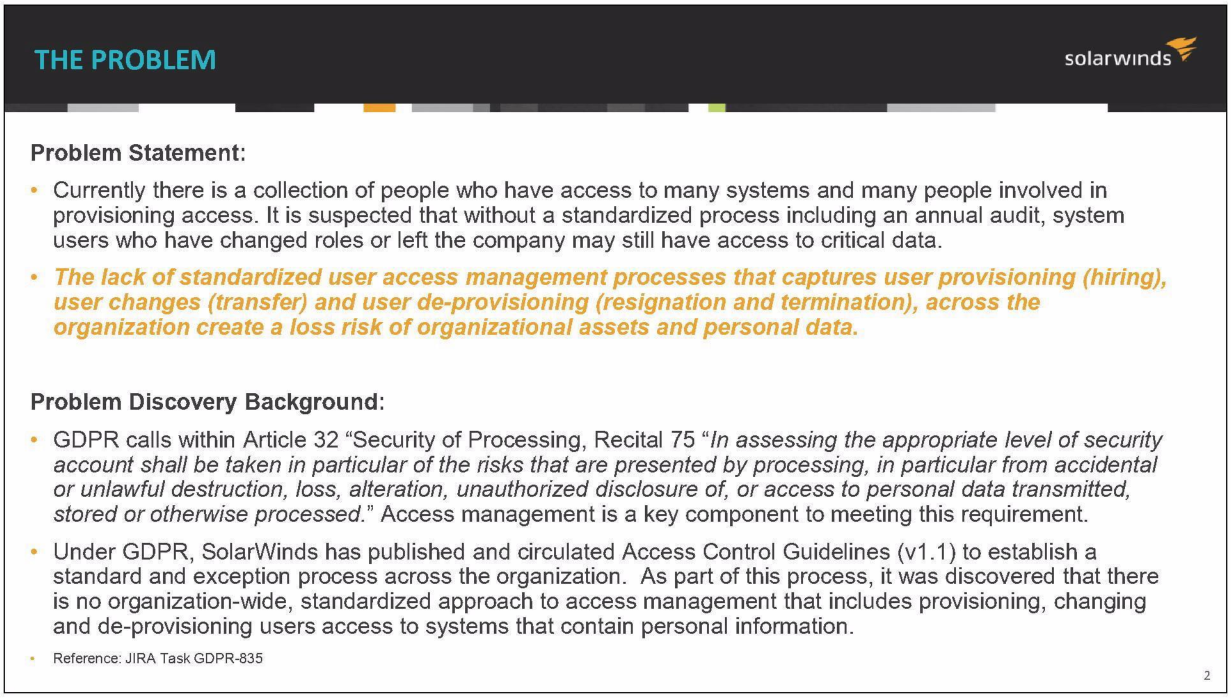
Thanks,
Kellie

solarwinds
Kellie Pierce | GDPR Project Manager | **SolarWinds**
Office: 512.498.6575

USER ACCESS MANAGEMENT

JANUARY 8, 2018

TOOL EVALUATION & RECOMMENDATION



THE PROBLEM

solarwinds

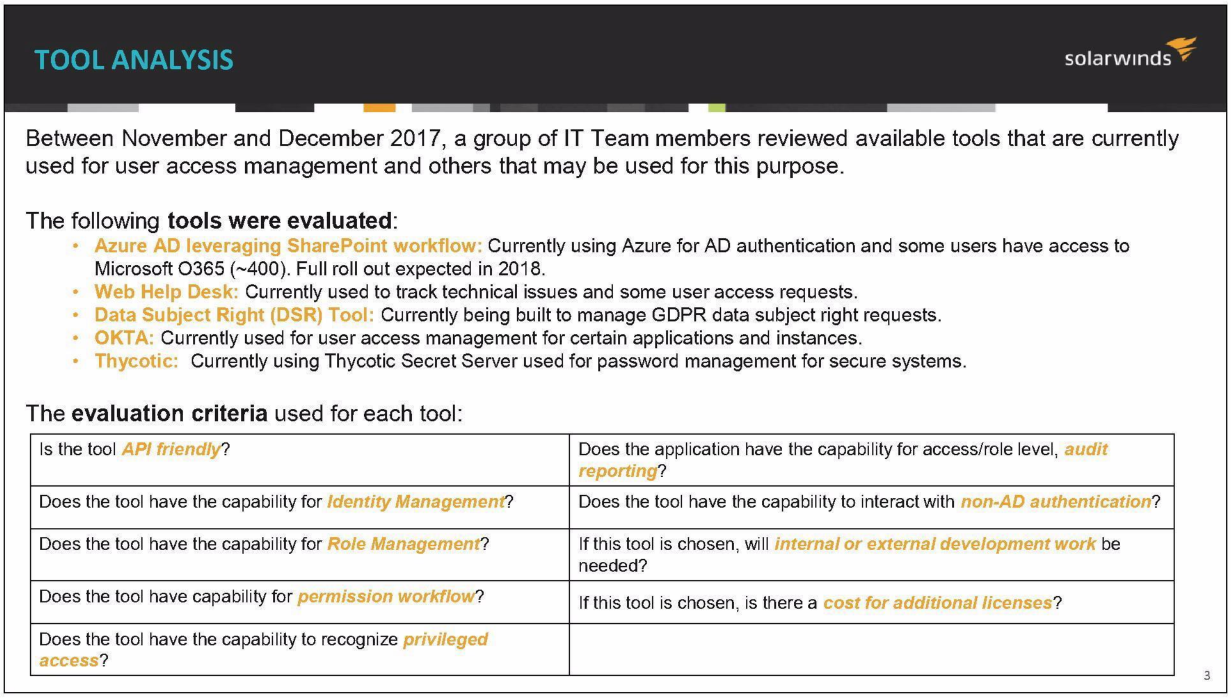
Problem Statement:

- Currently there is a collection of people who have access to many systems and many people involved in provisioning access. It is suspected that without a standardized process including an annual audit, system users who have changed roles or left the company may still have access to critical data.
- ***The lack of standardized user access management processes that captures user provisioning (hiring), user changes (transfer) and user de-provisioning (resignation and termination), across the organization create a loss risk of organizational assets and personal data.***

Problem Discovery Background:

- GDPR calls within Article 32 “Security of Processing, Recital 75 “*In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*” Access management is a key component to meeting this requirement.
- Under GDPR, SolarWinds has published and circulated Access Control Guidelines (v1.1) to establish a standard and exception process across the organization. As part of this process, it was discovered that there is no organization-wide, standardized approach to access management that includes provisioning, changing and de-provisioning users access to systems that contain personal information.
- Reference: JIRA Task GDPR-835

2



TOOL ANALYSIS

solarwinds

Between November and December 2017, a group of IT Team members reviewed available tools that are currently used for user access management and others that may be used for this purpose.

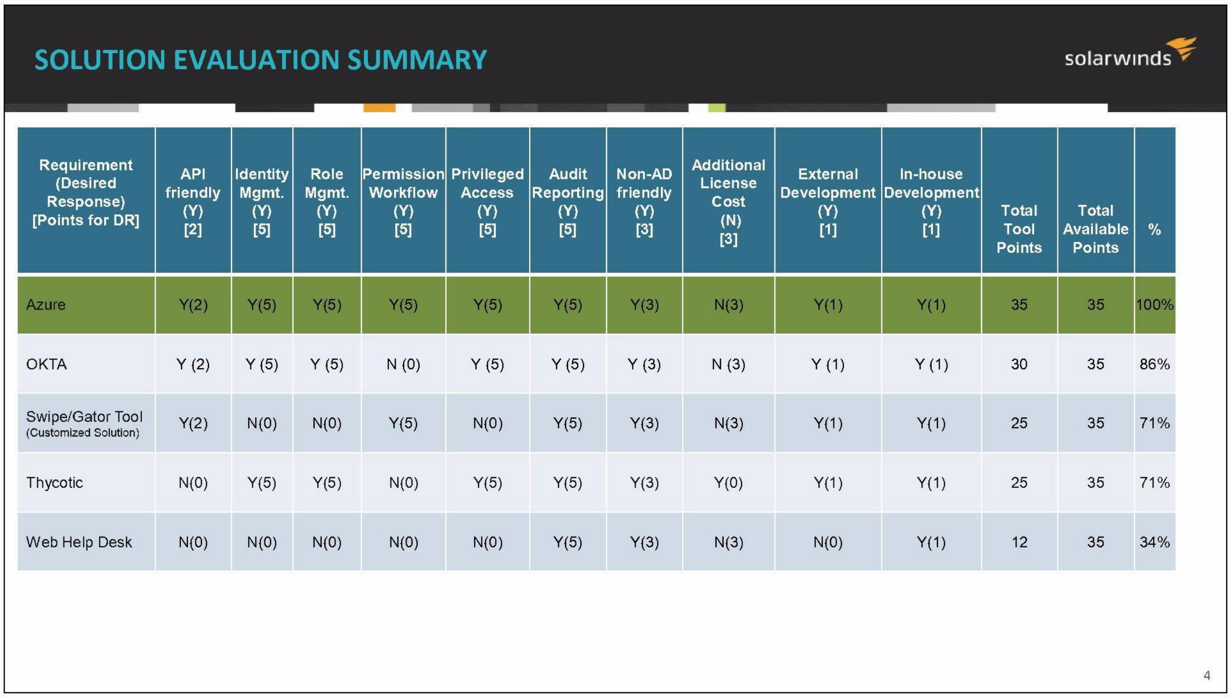
The following **tools were evaluated**:

- **Azure AD leveraging SharePoint workflow:** Currently using Azure for AD authentication and some users have access to Microsoft O365 (~400). Full roll out expected in 2018.
- **Web Help Desk:** Currently used to track technical issues and some user access requests.
- **Data Subject Right (DSR) Tool:** Currently being built to manage GDPR data subject right requests.
- **OKTA:** Currently used for user access management for certain applications and instances.
- **Thycotic:** Currently using Thycotic Secret Server used for password management for secure systems.

The **evaluation criteria** used for each tool:

Is the tool ***API friendly***?	Does the application have the capability for access/role level, ***audit reporting***?
Does the tool have the capability for ***Identity Management***?	Does the tool have the capability to interact with ***non-AD authentication***?
Does the tool have the capability for ***Role Management***?	If this tool is chosen, will ***internal or external development work*** be needed?
Does the tool have capability for ***permission workflow***?	If this tool is chosen, is there a ***cost for additional licenses***?
Does the tool have the capability to recognize ***privileged access***?	

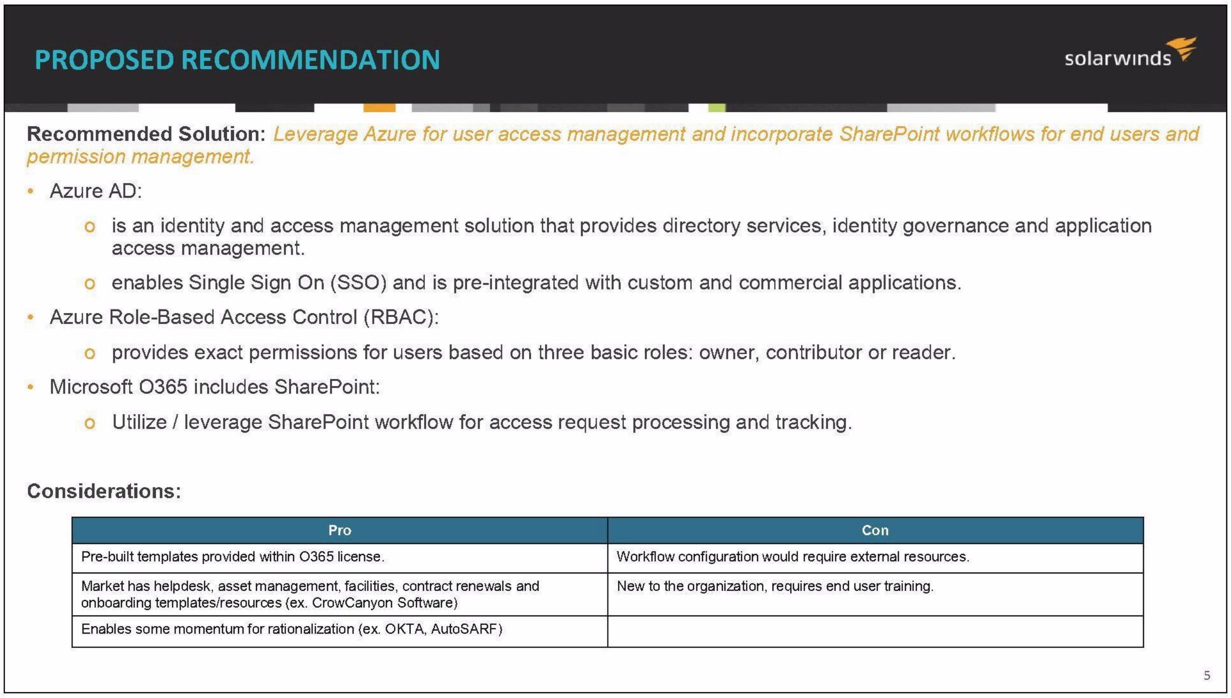
3



SOLUTION EVALUATION SUMMARY

solarwinds

Requirement (Desired Response) [Points for DR]	API friendly (Y) [2]	Identity Mgmt. (Y) [5]	Role Mgmt. (Y) [5]	Permission Workflow (Y) [5]	Privileged Access (Y) [5]	Audit Reporting (Y) [5]	Non-AD friendly (Y) [3]	Additional License Cost (N) [3]	External Development (Y) [1]	In-house Development (Y) [1]	Total Tool Points	Total Available Points	%
Azure	Y(2)	Y(5)	Y(5)	Y(5)	Y(5)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	35	35	100%
OKTA	Y (2)	Y (5)	Y (5)	N (0)	Y (5)	Y (5)	Y (3)	N (3)	Y (1)	Y (1)	30	35	86%
Swipe/Gator Tool (Customized Solution)	Y(2)	N(0)	N(0)	Y(5)	N(0)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	25	35	71%
Thycotic	N(0)	Y(5)	Y(5)	N(0)	Y(5)	Y(5)	Y(3)	Y(0)	Y(1)	Y(1)	25	35	71%
Web Help Desk	N(0)	N(0)	N(0)	N(0)	N(0)	Y(5)	Y(3)	N(3)	N(0)	Y(1)	12	35	34%



PROPOSED RECOMMENDATION

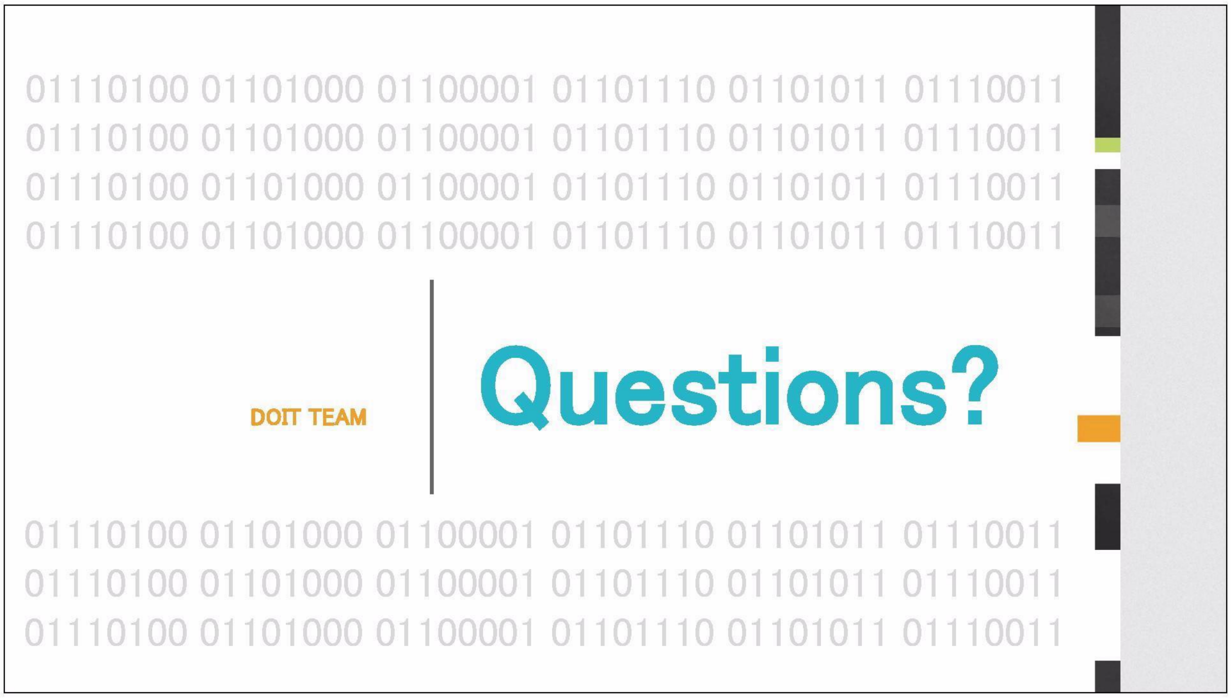
solarwinds

Recommended Solution: *Leverage Azure for user access management and incorporate SharePoint workflows for end users and permission management.*

- Azure AD:
  - is an identity and access management solution that provides directory services, identity governance and application access management.
  - enables Single Sign On (SSO) and is pre-integrated with custom and commercial applications.
- Azure Role-Based Access Control (RBAC):
  - provides exact permissions for users based on three basic roles: owner, contributor or reader.
- Microsoft O365 includes SharePoint:
  - Utilize / leverage SharePoint workflow for access request processing and tracking.

Considerations:

Pro	Con
Pre-built templates provided within O365 license.	Workflow configuration would require external resources.
Market has helpdesk, asset management, facilities, contract renewals and onboarding templates/resources (ex. CrowCanyon Software)	New to the organization, requires end user training.
Enables some momentum for rationalization (ex. OKTA, AutoSARF)	

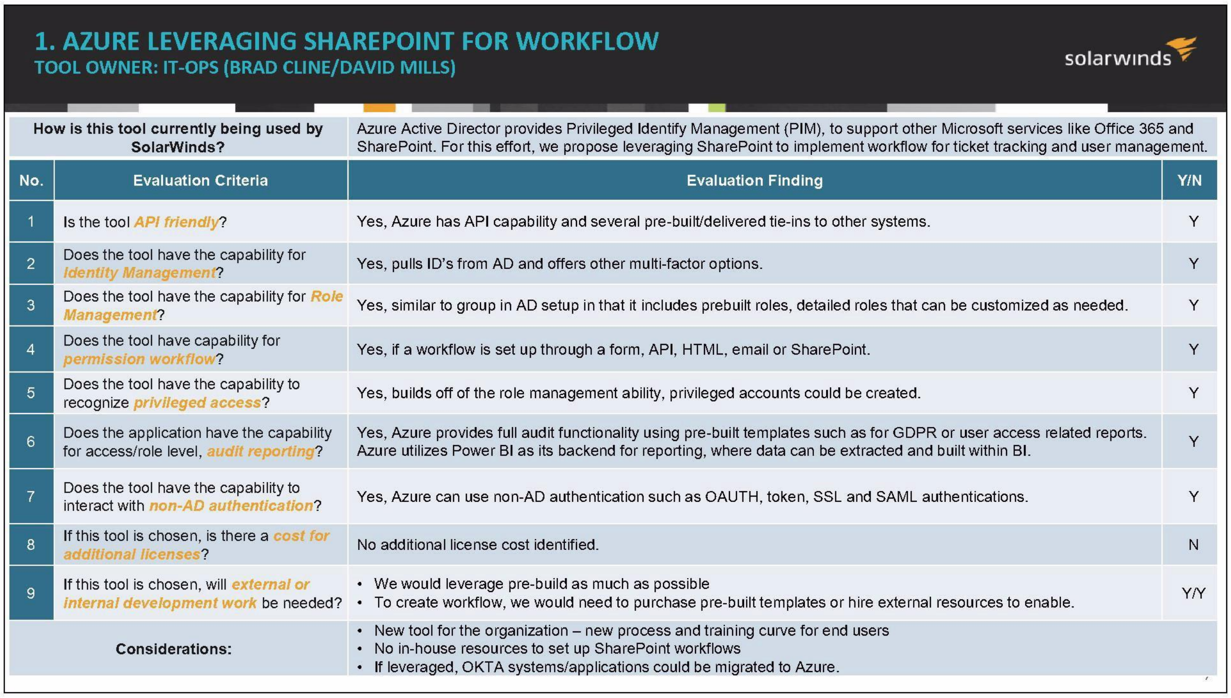


01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011

DOIT TEAM

Questions?

01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011

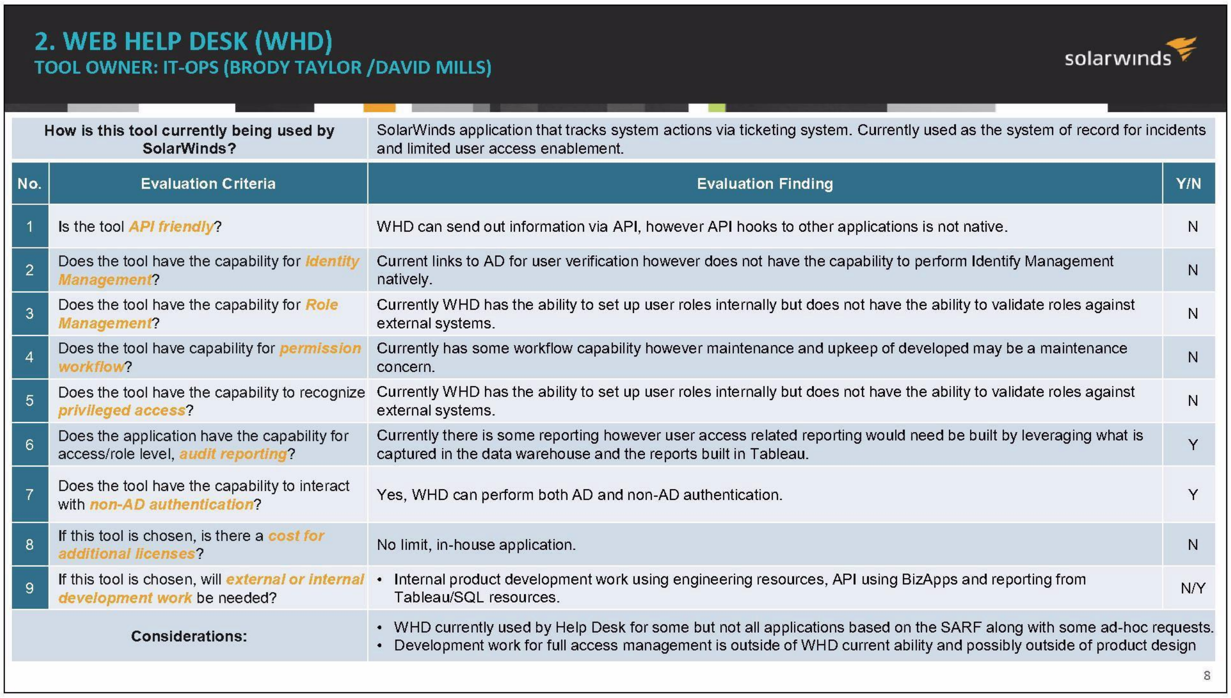


1. AZURE LEVERAGING SHAREPOINT FOR WORKFLOW

TOOL OWNER: IT-OPS (BRAD CLINE/DAVID MILLS)

solarwinds

How is this tool currently being used by SolarWinds?	Azure Active Director provides Privileged Identify Management (PIM), to support other Microsoft services like Office 365 and SharePoint. For this effort, we propose leveraging SharePoint to implement workflow for ticket tracking and user management.		
No.	**Evaluation Criteria**	**Evaluation Finding**	**Y/N**
1	Is the tool ***API friendly***?	Yes, Azure has API capability and several pre-built/delivered tie-ins to other systems.	Y
2	Does the tool have the capability for ***Identity Management***?	Yes, pulls ID's from AD and offers other multi-factor options.	Y
3	Does the tool have the capability for ***Role Management***?	Yes, similar to group in AD setup in that it includes prebuilt roles, detailed roles that can be customized as needed.	Y
4	Does the tool have capability for ***permission workflow***?	Yes, if a workflow is set up through a form, API, HTML, email or SharePoint.	Y
5	Does the tool have the capability to recognize ***privileged access***?	Yes, builds off of the role management ability, privileged accounts could be created.	Y
6	Does the application have the capability for access/role level, ***audit reporting***?	Yes, Azure provides full audit functionality using pre-built templates such as for GDPR or user access related reports. Azure utilizes Power BI as its backend for reporting, where data can be extracted and built within BI.	Y
7	Does the tool have the capability to interact with ***non-AD authentication***?	Yes, Azure can use non-AD authentication such as OAUTH, token, SSL and SAML authentications.	Y
8	If this tool is chosen, is there a ***cost for additional licenses***?	No additional license cost identified.	N
9	If this tool is chosen, will ***external or internal development work*** be needed?	• We would leverage pre-build as much as possible • To create workflow, we would need to purchase pre-built templates or hire external resources to enable.	Y/Y
Considerations:	• New tool for the organization – new process and training curve for end users • No in-house resources to set up SharePoint workflows • If leveraged, OKTA systems/applications could be migrated to Azure.		



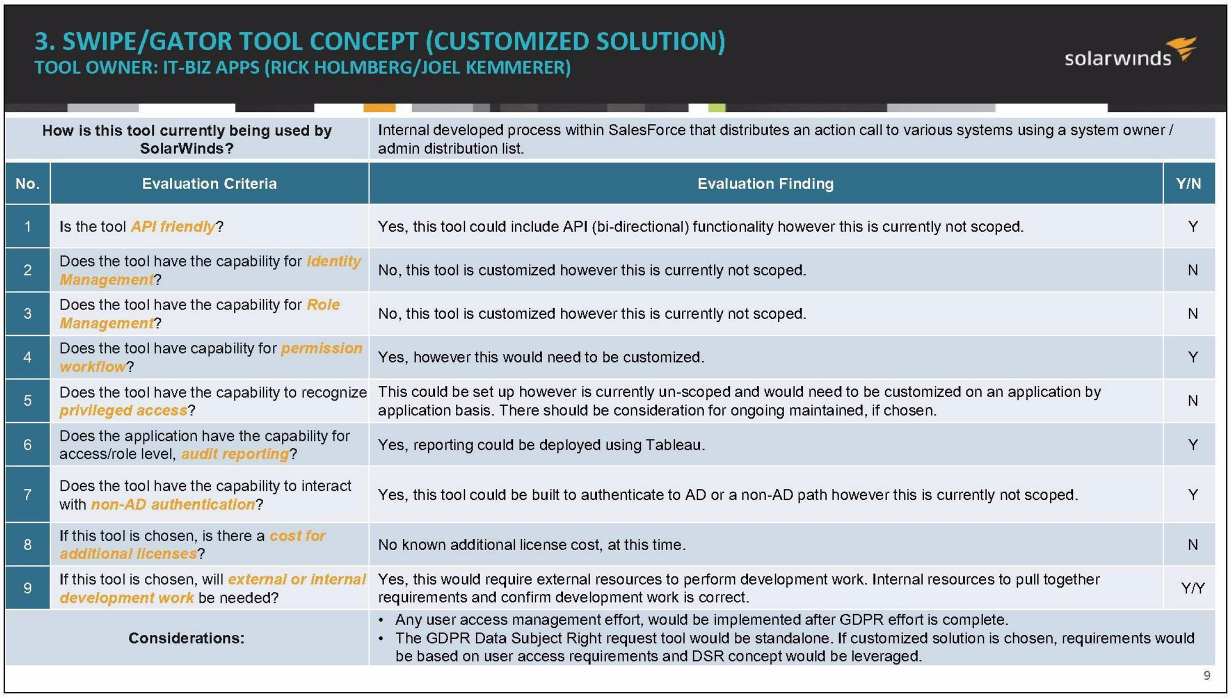
2. WEB HELP DESK (WHD)

TOOL OWNER: IT-OPS (BRODY TAYLOR /DAVID MILLS)

solarwinds

How is this tool currently being used by SolarWinds?		SolarWinds application that tracks system actions via ticketing system. Currently used as the system of record for incidents and limited user access enablement.	
No.	**Evaluation Criteria**	**Evaluation Finding**	**Y/N**
1	Is the tool ***API friendly***?	WHD can send out information via API, however API hooks to other applications is not native.	N
2	Does the tool have the capability for ***Identity Management***?	Current links to AD for user verification however does not have the capability to perform Identify Management natively.	N
3	Does the tool have the capability for ***Role Management***?	Currently WHD has the ability to set up user roles internally but does not have the ability to validate roles against external systems.	N
4	Does the tool have capability for ***permission workflow***?	Currently has some workflow capability however maintenance and upkeep of developed may be a maintenance concern.	N
5	Does the tool have the capability to recognize ***privileged access***?	Currently WHD has the ability to set up user roles internally but does not have the ability to validate roles against external systems.	N
6	Does the application have the capability for access/role level, ***audit reporting***?	Currently there is some reporting however user access related reporting would need be built by leveraging what is captured in the data warehouse and the reports built in Tableau.	Y
7	Does the tool have the capability to interact with ***non-AD authentication***?	Yes, WHD can perform both AD and non-AD authentication.	Y
8	If this tool is chosen, is there a ***cost for additional licenses***?	No limit, in-house application.	N
9	If this tool is chosen, will ***external or internal development work*** be needed?	• Internal product development work using engineering resources, API using BizApps and reporting from Tableau/SQL resources.	N/Y
Considerations:		• WHD currently used by Help Desk for some but not all applications based on the SARF along with some ad-hoc requests. • Development work for full access management is outside of WHD current ability and possibly outside of product design	

8



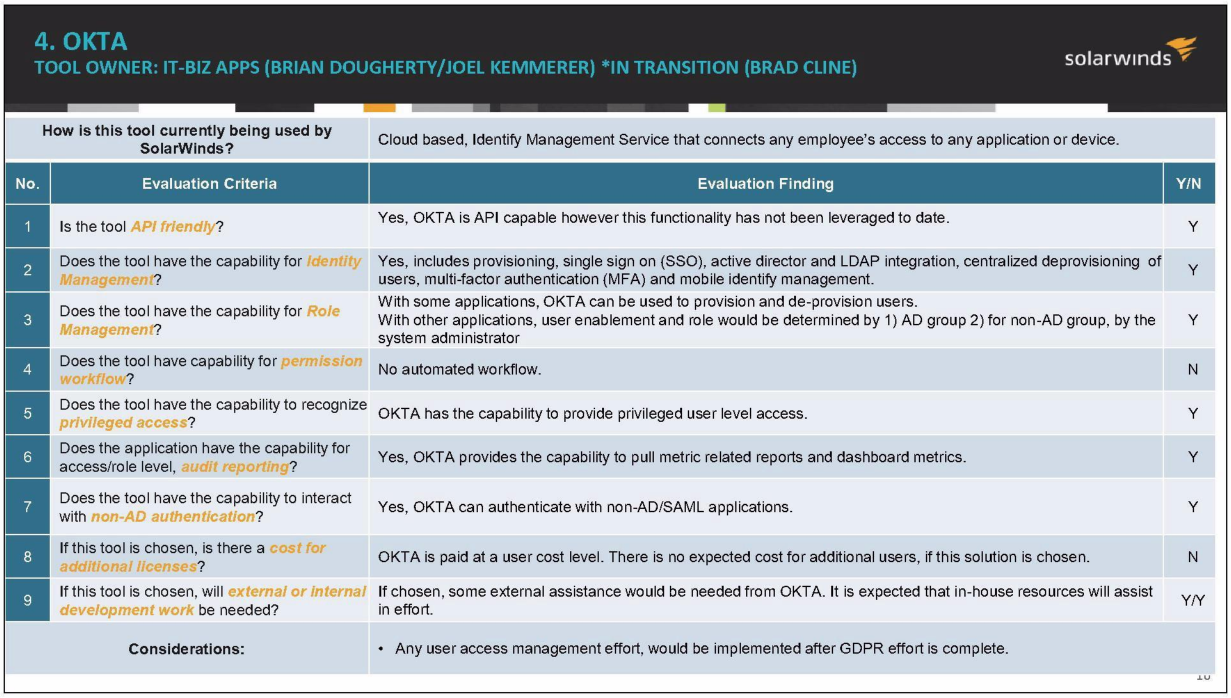
3. SWIPE/GATOR TOOL CONCEPT (CUSTOMIZED SOLUTION)

TOOL OWNER: IT-BIZ APPS (RICK HOLMBERG/JOEL KEMMERER)

solarwinds

How is this tool currently being used by SolarWinds?		Internal developed process within SalesForce that distributes an action call to various systems using a system owner / admin distribution list.	
No.	**Evaluation Criteria**	**Evaluation Finding**	**Y/N**
1	Is the tool ***API friendly***?	Yes, this tool could include API (bi-directional) functionality however this is currently not scoped.	Y
2	Does the tool have the capability for ***Identity Management***?	No, this tool is customized however this is currently not scoped.	N
3	Does the tool have the capability for ***Role Management***?	No, this tool is customized however this is currently not scoped.	N
4	Does the tool have capability for ***permission workflow***?	Yes, however this would need to be customized.	Y
5	Does the tool have the capability to recognize ***privileged access***?	This could be set up however is currently un-scoped and would need to be customized on an application by application basis. There should be consideration for ongoing maintained, if chosen.	N
6	Does the application have the capability for access/role level, ***audit reporting***?	Yes, reporting could be deployed using Tableau.	Y
7	Does the tool have the capability to interact with ***non-AD authentication***?	Yes, this tool could be built to authenticate to AD or a non-AD path however this is currently not scoped.	Y
8	If this tool is chosen, is there a ***cost for additional licenses***?	No known additional license cost, at this time.	N
9	If this tool is chosen, will ***external or internal development work*** be needed?	Yes, this would require external resources to perform development work. Internal resources to pull together requirements and confirm development work is correct.	Y/Y
Considerations:		• Any user access management effort, would be implemented after GDPR effort is complete. • The GDPR Data Subject Right request tool would be standalone. If customized solution is chosen, requirements would be based on user access requirements and DSR concept would be leveraged.	

9

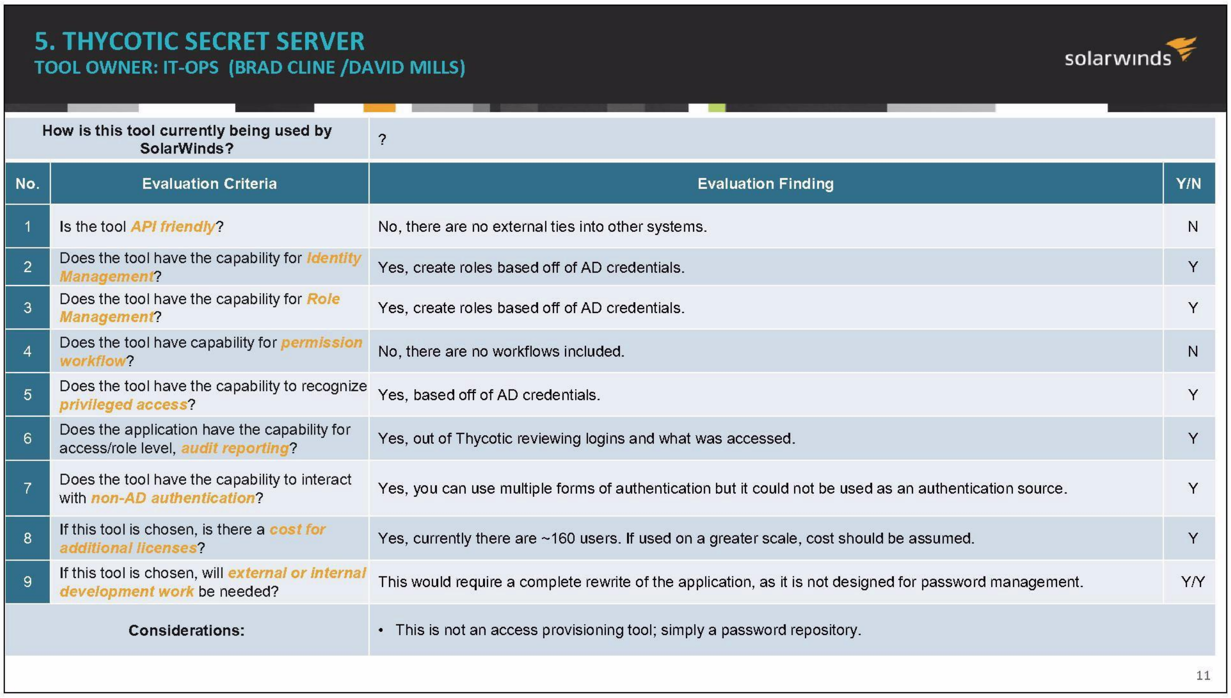


4. OKTA

TOOL OWNER: IT-BIZ APPS (BRIAN DOUGHERTY/JOEL KEMMERER) *IN TRANSITION (BRAD CLINE)

solarwinds

How is this tool currently being used by SolarWinds?		Cloud based, Identify Management Service that connects any employee's access to any application or device.	
No.	**Evaluation Criteria**	**Evaluation Finding**	**Y/N**
1	Is the tool ***API friendly***?	Yes, OKTA is API capable however this functionality has not been leveraged to date.	Y
2	Does the tool have the capability for ***Identity Management***?	Yes, includes provisioning, single sign on (SSO), active director and LDAP integration, centralized deprovisioning of users, multi-factor authentication (MFA) and mobile identify management.	Y
3	Does the tool have the capability for ***Role Management***?	With some applications, OKTA can be used to provision and de-provision users. With other applications, user enablement and role would be determined by 1) AD group 2) for non-AD group, by the system administrator	Y
4	Does the tool have capability for ***permission workflow***?	No automated workflow.	N
5	Does the tool have the capability to recognize ***privileged access***?	OKTA has the capability to provide privileged user level access.	Y
6	Does the application have the capability for access/role level, ***audit reporting***?	Yes, OKTA provides the capability to pull metric related reports and dashboard metrics.	Y
7	Does the tool have the capability to interact with ***non-AD authentication***?	Yes, OKTA can authenticate with non-AD/SAML applications.	Y
8	If this tool is chosen, is there a ***cost for additional licenses***?	OKTA is paid at a user cost level. There is no expected cost for additional users, if this solution is chosen.	N
9	If this tool is chosen, will ***external or internal development work*** be needed?	If chosen, some external assistance would be needed from OKTA. It is expected that in-house resources will assist in effort.	Y/Y
Considerations:		• Any user access management effort, would be implemented after GDPR effort is complete.	



5. THYCOTIC SECRET SERVER

TOOL OWNER: IT-OPS (BRAD CLINE /DAVID MILLS)

solarwinds

How is this tool currently being used by SolarWinds?	?		
No.	**Evaluation Criteria**	**Evaluation Finding**	**Y/N**
1	Is the tool ***API friendly***?	No, there are no external ties into other systems.	N
2	Does the tool have the capability for ***Identity Management***?	Yes, create roles based off of AD credentials.	Y
3	Does the tool have the capability for ***Role Management***?	Yes, create roles based off of AD credentials.	Y
4	Does the tool have capability for ***permission workflow***?	No, there are no workflows included.	N
5	Does the tool have the capability to recognize ***privileged access***?	Yes, based off of AD credentials.	Y
6	Does the application have the capability for access/role level, ***audit reporting***?	Yes, out of Thycotic reviewing logins and what was accessed.	Y
7	Does the tool have the capability to interact with ***non-AD authentication***?	Yes, you can use multiple forms of authentication but it could not be used as an authentication source.	Y
8	If this tool is chosen, is there a ***cost for additional licenses***?	Yes, currently there are ~160 users. If used on a greater scale, cost should be assumed.	Y
9	If this tool is chosen, will ***external or internal development work*** be needed?	This would require a complete rewrite of the application, as it is not designed for password management.	Y/Y
Considerations:	- This is not an access provisioning tool; simply a password repository.		